Silverfort | servicenow

Silverfort and ServiceNow: Just-in-Time access with ticket-based approval validation

As organizations modernize their identity security programs, controlling privileged access remains a critical challenge. IT Service Management (ITSM) platforms like ServiceNow play a key role in managing approval workflows and operational processes across the organization. Silverfort extends these workflows by connecting approved access requests to enforcement at runtime, ensuring that privileged access is not only approved, but also validated and controlled at the moment it occurs.

Enforcing approved access at runtime

The Silverfort and ServiceNow integration enables organizations to enforce ticket-based approval validation directly within privileged access workflows. Instead of relying on manual processes or post-approval checks, Silverfort ensures that access is granted only when it is:

- Approved through ServiceNow workflows
- Requested by the correct user
- Still valid and within the approved timeframe

By correlating Silverfort's identity intelligence with network, endpoint, and cloud activity inside QRadar, security teams can identify compromised users and systems faster, reduce investigation time, and focus on the most critical incidents.

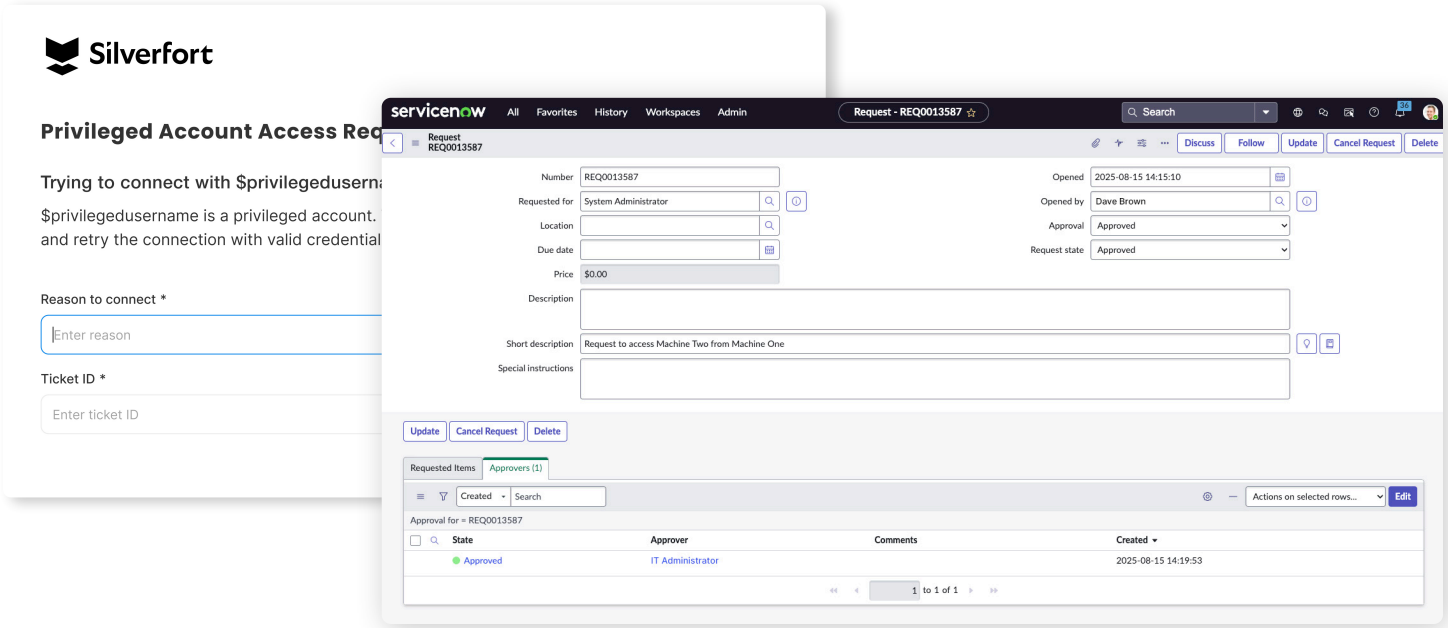
How it works

When a user requests privileged access through Silverfort's Just-in-Time (JIT) workflow, the request is validated against an approved ServiceNow ticket before access is granted.

How it works (continued)

Silverfort verifies that the request is associated with a valid and approved ticket, ensures the requesting user matches the approved identity, and confirms that the approval is still relevant. Only after successful validation does Silverfort grant privileged access, enforcing security controls at runtime.

This ensures that every privileged session is tied to an authorized request, preventing misuse, reducing risk, and aligning access enforcement with existing ServiceNow approval workflows.



Key benefits

Prevent privileged access abuse

Block unauthorized or misaligned access requests – including stale or improperly used tickets – to reduce the risk of privilege misuse and lateral movement.

Align Identity Security with ITSM workflows

Leverage existing ServiceNow approval processes without changing how teams request or approve access.

Enforce approved privileged access

Ensure every privileged session is tied to a valid, approved ServiceNow request before access is granted.

Strengthen identity accountability

Validate that access is granted only to the correct user, ensuring clear ownership and auditability of privileged actions.

Reduce operational risk

Eliminate gaps between approval and enforcement, ensuring access is always controlled at the moment it occurs.

About Silverfort

Silverfort secures every dimension of identity. We deliver end-to-end identity security that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity, analyze exposures, and enforce protection inline to stop lateral movement, ransomware, and other identity threats.